doi:10.1006/jabr.2000.8454, available online at http://www.idealibrary.com on IDEAL

On a Power Integral Bases Problem over Cyclotomic $\mathbf{Z}_p$-Extensions

Humio Ichimura[1]

Department of Mathematics, Yokohama City University, 22-2, Seto, Kanazawa-ku, Yokohama 236-0027, Japan

Communicated by Walter Feit

Received June 29, 1999

1. INTRODUCTION

This is a continuation of the paper [10]. For a finite extension L/K of a number field K, one says that it has a relative power integral basis (PIB for short) when $O_L = O_K[\alpha]$ for some $\alpha \in O_L$. Here, O_L (resp. O_K) is the ring of integers of L (resp. K). We say that L/K is "unramified" when it is unramified at all finite prime divisors. Let p be a fixed prime number and let K be a number field containing a primitive pth root ζ_p of unity. In [10], we gave a proof of the following theorem.

THEOREM 1 (Kawamoto, Suwa, and the author). *An unramified cyclic extension L/K of degree p has a PIB if $L = K(\epsilon^{1/p})$ for some unit ϵ of K.*

Denote by E_K the group of units of K. Let $\mathscr{H}(K)$ be the subgroup of $K^\times/(K^\times)^p$ consisting of classes $[\alpha]$ ($\alpha \in K^\times$) for which $K(\alpha^{1/p})/K$ is unramified, and let $\mathscr{E}(K) = \mathscr{H}(K) \cap E_K(K^\times)^p/(K^\times)^p$. In view of Theorem 1, the quotient group $\mathscr{H}(K)/\mathscr{E}(K)$ is naturally of interest. Let $p \geq 3$ and let K be a CM-field with $\zeta_p \in K$. By the action of the complex conjugation, we can decompose the groups $\mathscr{H}(K)$, $\mathscr{E}(K)$ as $\mathscr{H}(K) = \mathscr{H}(K)^+ \oplus \mathscr{H}(K)^-$, etc. Assume, for the moment, that p does not divide the class number $h^+ = h(K^+)$ of the maximal real subfield K^+ of K. Then we have $\mathscr{H}(K) = \mathscr{H}(K)^+ = \mathscr{E}(K)^+$ by [10, Proposition 2]. In particular, every unramified cyclic extension over K of degree p has a PIB.

[1] Partially supported by Grant-in-Aid for Scientific Research (C), Grant 11640041.

0021-8693/00 $35.00

In this paper, we prove assertions on $\mathscr{H}(K)^+/\mathscr{E}(K)^+$, without assuming $p \nmid h^+$, when K is a sufficiently high layer of the cyclotomic $\boldsymbol{Z}_p$-extension of an imaginary abelian field. Let p be a fixed odd prime number and let k be an imaginary abelian field with $\zeta_p \in k$. Let k_∞/k be the cyclotomic $\boldsymbol{Z}_p$-extension with its nth layer $k_n (n \geq 0)$, and let k_∞^+ and k_n^+ be the corresponding objects for the maximal real subfield k^+. We write $\mathscr{H}_n = \mathscr{H}(k_n)$ and $\mathscr{E}_n = \mathscr{E}(k_n)$ for brevity. Denote by λ_k and λ_k^+ the Iwasawa λ-invariants of the ideal class groups of k_∞ and k_∞^+, respectively, and put $\lambda_k^- = \lambda_k - \lambda_k^+$. It is conjectured that $\lambda_k^+ = 0$ (cf. Greenberg [6]). We have many numerical examples with $\lambda_k^+ = 0$ but no counterexamples (see [12] and its references). It is known that $\dim \mathscr{H}_n^+ = \lambda_k^-$ for all sufficiently large n (see Section 6). Here, $\dim(*)$ denotes the dimension of a vector space over the prime field $\boldsymbol{Z}/p\boldsymbol{Z}$. Our first result for $\mathscr{H}_n^+/\mathscr{E}_n^+$ is the following:

PROPOSITION 1. *Under the above setting, assume that $\lambda_k^+ = 0$. Then there exists an integer n_0 such that $\mathscr{H}_n^+/\mathscr{E}_n^+ = \{0\}$ for all $n \geq n_0$.*

Using the Kummer duality, we obtain the following theorem from Proposition 1 and Theorem 1.

THEOREM 2. *Let p, k, and n_0 be as in Proposition 1. Let n be an integer with $n \geq n_0$ and let L/k_n be an unramified cyclic extension of degree p such that L is Galois over k_n^+ and the complex conjugation of k_n acts on* $\mathrm{Gal}(L/k_n)$ *via* (-1)*-multiplication. Then, L/k_n has a PIB.*

Further, we prove the following quantitative version of Proposition 1. Assume that $p \nmid [k : \boldsymbol{Q}]$. We put $\Delta = \mathrm{Gal}(k/\boldsymbol{Q})$, which we regard as a subgroup of $\mathrm{Gal}(k_\infty/\boldsymbol{Q})$ in the usual way. A $\boldsymbol{Q}_p$-valued character of Δ defined and irreducible over $\boldsymbol{Q}_p$ is simply called a $\boldsymbol{Q}_p$-character. Let Ψ be a fixed nontrivial *even* $\boldsymbol{Q}_p$-character of Δ, and let ψ be a fixed irreducible component of Ψ over an algebraic closure $\overline{\boldsymbol{Q}}_p$ of $\boldsymbol{Q}_p$. Here, we say that Ψ is even when $\psi(\rho) = 1$, ρ being the complex conjugation in Δ. Denote by λ_Ψ and $(\mathscr{H}_n/\mathscr{E}_n)(\Psi)$ the Ψ-components of λ_k^+ and $\mathscr{H}_n/\mathscr{E}_n$, respectively. (For the definitions, see Section 3.1.)

THEOREM 3. *Under the above setting, we assume that $p \nmid [k : \boldsymbol{Q}]$ and that $\psi(p) \neq 1$ regarding ψ as a primitive Dirichlet character. Then we have*

$$\dim(\mathscr{H}_n/\mathscr{E}_n)(\Psi) = \lambda_\Psi \cdot \deg(\Psi)$$

for all sufficiently large n. Here, $\deg(\Psi)$ *denotes the degree of* Ψ.

Remark 1. Theorem 1 was proved independently by F. Kawamoto, N. Suwa, and the author by methods different from each other. For details, see [10, Remark 3].

Remark 2. An effective method to calculate (an upper bound of) the integer n_0 in Proposition 1 (and, at the same time, show $\lambda_k^+ = 0$) is established in [11] for a certain class of abelian fields.

Remark 3. (1) When Ψ is the trivial character Ψ_0, we have $\mathcal{H}_n(\Psi_0) = \{0\}$ and $\lambda_{\Psi_0} = 0$ by the Stickelberger theorem (cf. [9, Remark 1(2)]). (2) We have $\lambda_k^+ = \sum_\Psi \lambda_\Psi \cdot \deg(\Psi)$, where Ψ runs over all even $\boldsymbol{Q}_p$-characters of Δ. (3) The assumption $\psi(p) \neq 1$ in Theorem 3 is essential in our argument. For details, see Remark 6 in Section 5.

The content of this paper is as follows. We prove Proposition 1 and Theorem 2 in Section 2. In Section 3, we prove Theorem 3 after introducing some assertions (Propositions 2, 3, and 4) on several "unramified" abelian extensions over k_∞. We prove these key propositions in Sections 4 and 5. In Section 6, we give some related topics and examples.

2. PROOF OF THEOREM 2

We begin with some preliminaries. Let p be a fixed odd prime number and let k be an imaginary abelian field with $\zeta_p \in k$. We regard $\Delta = \mathrm{Gal}(k/\boldsymbol{Q})$ as a subgroup of $\mathrm{Gal}(k_\infty/\boldsymbol{Q})$ in the usual way. Let A_n be the Sylow p-subgroup of the ideal class group of k_n. Denote by $A_\infty, \mathcal{H}_\infty, \mathcal{E}_\infty$ the inductive limits of $A_n, \mathcal{H}_n, \mathcal{E}_n$ with respect to the inclusion maps $k_n \to k_m (n \leq m)$, respectively:

$$A_\infty = \varinjlim A_n, \qquad \mathcal{H}_\infty = \varinjlim \mathcal{H}_n, \qquad \mathcal{E}_\infty = \varinjlim \mathcal{E}_n.$$

These groups are naturally regarded as modules over the group ring $\boldsymbol{Z}_p[\Delta]$. For a $\boldsymbol{Z}_p[\Delta]$-module X, we decompose it as $X = X^+ \oplus X^-$ by the action of the complex conjugation. By a theorem of Ferrero and Washington [4], we see that $\mathcal{H}_\infty$ is a finite abelian group, and hence that

$$\mathcal{H}_\infty/\mathcal{E}_\infty = \mathcal{H}_n/\mathcal{E}_n \qquad \text{for all sufficiently large } n \tag{1}$$

regarding $\mathcal{H}_n$ as a subgroup of $\mathcal{H}_\infty$ via the inclusion map $k_n^\times \to k_\infty^\times$. For each element $[\alpha] \in \mathcal{H}_n$ with $\alpha \in k_n^\times$, there exists an ideal $\mathfrak{A}$ of k_n such that $\mathfrak{A}^p = (\alpha)$. By mapping $[\alpha]$ to the class of $\mathfrak{A}$, we obtain the following exact sequence compatible with the Δ-action:

$$0 \longrightarrow \mathcal{E}_n \longrightarrow \mathcal{H}_n \longrightarrow A_n.$$

From this, we obtain the exact sequence

$$0 \longrightarrow \mathcal{E}_\infty \longrightarrow \mathcal{H}_\infty \longrightarrow A_\infty. \tag{2}$$

Let L_n be the Hilbert p-class field of k_n, and $\mathfrak{X}_n = \mathrm{Gal}(L_n/k_n)$. We regard $\mathfrak{X}_n$ as a module over Δ. The Kummer pairing

$$\mathfrak{X}_n/\mathfrak{X}_n^p \times \mathscr{H}_n \longrightarrow \mu_p \tag{3}$$

is defined by

$$\langle [\sigma], [\alpha] \rangle = (\alpha^{1/p})^{\sigma - 1}$$

for $\sigma \in \mathfrak{X}_n$ and $[\alpha] \in \mathscr{H}_n$. This enjoys the property

$$\langle [\sigma]^\rho, [\alpha]^\rho \rangle = \langle [\sigma], [\alpha] \rangle^\rho = \langle [\sigma], [\alpha] \rangle^{\omega(\rho)} \tag{4}$$

for $\rho \in \Delta$, where ω is the character of Δ representing the Galois action on pth roots of unity.

Proof of Proposition 1. Assume that $\lambda_k^+ = 0$. This is equivalent to the condition $A_\infty^+ = \{0\}$ by [6, Proposition 2]. Hence, we obtain $\mathscr{H}_\infty^+ = \mathscr{E}_\infty^+$ by (2). Therefore, we obtain the assertion by (1). ∎

Proof of Theorem 2. From the above Kummer pairing and (4), we obtain the perfect pairing

$$\mathfrak{X}_n^-/(\mathfrak{X}_n^-)^p \times \mathscr{H}_n^+ \longrightarrow \mu_p.$$

From this, Proposition 1, and Theorem 1, the assertion follows. ∎

3. PROOF OF THEOREM 3

3.1. *Several Unramified Abelian Extensions over* k_∞

Let p and k be as in Section 2. Denote by E_n the group of units of k_n: $E_n = E_{k_n}$. Let M/k_∞ be the maximal pro-p abelian extension unramified outside p, let L/k_∞ be the maximal unramified pro-p abelian extension, and let

$$N = \bigcup_n k_\infty(\epsilon^{1/p^{n+1}} \mid \epsilon \in E_n).$$

We put

$$\mathfrak{G} = \mathrm{Gal}(M/k_\infty),\ \mathfrak{H} = \mathrm{Gal}(N/k_\infty),$$

$$\mathfrak{X} = \mathrm{Gal}(L/k_\infty),\ \mathfrak{Y} = \mathrm{Gal}(N \cap L/k_\infty).$$

These groups as well as $\mathscr{H}_n$, etc., are naturally regarded as $\boldsymbol{Z}_p[\Delta]$-modules. Denote by M^+ (resp. M^-) the intermediate field of M/k_∞ corresponding to $\mathfrak{G}^-$ (resp. $\mathfrak{G}^+$) by Galois theory. Hence, we have $\mathrm{Gal}(M^\pm/k_\infty) = \mathfrak{G}^\pm$. We put $F^+ = F \cap M^+$ and $F^- = F \cap M^-$ for an intermediate field F of M/k_∞ which is Galois also over k_∞^+. The following assertion is more or less known.

PROPOSITION 2. *Under the above setting, the following hold*:

(a) $\mathrm{Gal}(M^-/N^-) \cong \mathrm{Hom}(A_\infty^+, \mu_{p^\infty})$ *over* $\boldsymbol{Z}_p$.

(b) $M^- = N^- L^-$.

To prove Theorem 3, we need the Δ-decomposed version of Proposition 2. In what follows, we always assume that $p \nmid [k : \boldsymbol{Q}]$. Let Φ be a $\boldsymbol{Q}_p$-character of $\Delta = \mathrm{Gal}(k/\boldsymbol{Q})$ and let

$$e_\Phi = \frac{1}{|\Delta|} \sum_{\sigma \in \Delta} \Phi(\sigma)\sigma^{-1}$$

be the idempotent of Φ. We have $e_\Phi \in \boldsymbol{Z}_p[\Delta]$ as $p \nmid [k : \boldsymbol{Q}]$. For a $\boldsymbol{Z}_p[\Delta]$-module X, we denote by $X(\Phi)$ the Φ-component $e_\Phi X$ (or X^{e_Φ}) of X. Let Ψ (resp. ψ) be, as before, a fixed nontrivial *even* $\boldsymbol{Q}_p$-character of Δ (resp. its irreducible component over $\overline{\boldsymbol{Q}}_p$). Let Ψ^* and ψ^* be the dual characters of Ψ and ψ defined respectively by

$$\Psi^*(\sigma) = \omega(\sigma)\Psi(\sigma^{-1}) \qquad \text{and} \qquad \psi^*(\sigma) = \omega(\sigma)\psi(\sigma^{-1}) \qquad (\sigma \in \Delta).$$

Here, ω is, as before, the character of Δ representing the Galois action on pth roots of unity. Denote by $M(\Psi^*)$ the intermediate field of M/k_∞ corresponding to $\bigoplus^* \mathfrak{G}(\Phi)$ by Galois theory where Φ runs over all $\boldsymbol{Q}_p$-characters of Δ with $\Phi \neq \Psi^*$. Hence, we have $\mathrm{Gal}(M(\Psi^*)/k_\infty) = \mathfrak{G}(\Psi^*)$. Define $N(\Psi^*)$, $L(\Psi^*)$, and $(N \cap L)(\Psi^*)$ in a similar way. Let O be the subring of $\overline{\boldsymbol{Q}}_p$ generated by the values of ψ over $\boldsymbol{Z}_p$. We identify the subring $e_\Psi \boldsymbol{Z}_p[\Delta]$ (resp. $e_{\Psi^*}\boldsymbol{Z}_p[\Delta]$) of $\boldsymbol{Z}_p[\Delta]$ with O by

$$e_\Psi(\sigma) \longrightarrow \psi(\sigma) \qquad (\textit{resp. } e_{\Psi^*}(\sigma) \longrightarrow \psi^*(\sigma)) \qquad (\sigma \in \Delta).$$

Hence, for a $\boldsymbol{Z}_p[\Delta]$-module X, we may regard $X(\Psi)$ and $X(\Psi^*)$ as O-modules. Further, we regard $H = \mathrm{Hom}(X, \mu_{p^\infty})$ as a $\boldsymbol{Z}_p[\Delta]$-module by

$$f^\sigma(x) = (f(x^{\sigma^{-1}}))^\sigma \qquad (f \in H,\ \sigma \in \Delta,\ x \in X).$$

Then its Ψ^*-component $H(\Psi^*) = \mathrm{Hom}(X(\Psi), \mu_{p^\infty})$ is also regarded as an O-module. The following is the Δ-decomposed version of Proposition 2, which is also more or less known.

PROPOSITION 3. *Under the above setting, the following hold*:

(a) $\mathrm{Gal}(M(\Psi^*)/N(\Psi^*)) \cong \mathrm{Hom}(A_\infty(\Psi), \mu_{p^\infty})$ *over* O.

(b) $M(\Psi^*) = N(\Psi^*)L(\Psi^*)$.

It follows from [4] that $\mathfrak{X}(\Psi^*)$ and the O-modules in (a) of the above proposition are finitely generated over O. For a finitely generated O-module X, we denote by $\operatorname{rank}_O X$ the dimension of the vector space $X \otimes_O Q$ over Q, Q being the quotient field of O. By definition, we have

$$\lambda_\Psi = \operatorname{rank}_O \operatorname{Hom}(A_\infty(\Psi), \mu_{p^\infty}). \tag{5}$$

Hence, from Proposition 3, we obtain

$$\lambda_\Psi = \operatorname{rank}_O \operatorname{Gal}\big(L(\Psi^*)/(N \cap L)(\Psi^*)\big). \tag{6}$$

It is known that $\mathfrak{X}(\Psi^*)$ is (finitely generated and) free over O as Ψ^* is odd (cf. Washington [15, Corollary 13.29]). On the quotient $\mathfrak{Y}(\Psi^*) = \operatorname{Gal}((N \cap L)(\Psi^*)/k_\infty)$ of $\mathfrak{X}(\Psi^*)$, we prove in Section 5 the following:

PROPOSITION 4. *When $\psi(p) \neq 1$, $\mathfrak{Y}(\Psi^*)$ is (finitely generated and) free over O.*

3.2. *Proof of Theorem* 3.

We use the same notation as before. Assume that $\psi(p) \neq 1$. We have an exact sequence of the free O-modules:

$$0 \longrightarrow \operatorname{Gal}\big(L(\Psi^*)/(N \cap L)(\Psi^*)\big) \longrightarrow \mathfrak{X}(\Psi^*) \longrightarrow \mathfrak{Y}(\Psi^*) \longrightarrow 0.$$

By the freeness, we obtain

$$\deg(\Psi^*) \cdot \operatorname{rank}_O \mathfrak{X}(\Psi^*) = \dim\big((\mathfrak{X}/\mathfrak{X}^p)(\Psi^*)\big) \tag{7}$$

$$\deg(\Psi^*) \cdot \operatorname{rank}_O \mathfrak{Y}(\Psi^*) = \dim\big((\mathfrak{Y}/\mathfrak{Y}^p)(\Psi^*)\big). \tag{8}$$

The Kummer pairing

$$\mathfrak{X}/\mathfrak{X}^p \times \mathscr{H}_\infty \longrightarrow \mu_p$$

is defined similarly to the pairing (3) and has the same property (4). From this, we see that the RHS of (7) and (8) are equal to $\dim \mathscr{H}_\infty(\Psi)$ and $\dim \mathscr{E}_\infty(\Psi)$, respectively. Therefore, we obtain

$$\dim(\mathscr{H}_\infty/\mathscr{E}_\infty)(\Psi) = \lambda_\Psi \cdot \deg(\Psi)$$

from the above exact sequence and (6). Theorem 3 follows from this and (1). ∎

4. PROOF OF PROPOSITIONS 2 AND 3

The assertions (a) of these propositions are proved exactly similarly to [13, Theorem 14]. So, we only prove the assertions (b).

Let k be an imaginary abelian field with $\zeta_p \in k$ but not neccesarily satisfying $p \nmid [k : \boldsymbol{Q}]$, and let $\Gamma = \mathrm{Gal}(k_\infty/k)$. We fix a topological generator γ of Γ once and for all, and identify, as usual, the completed group ring $\boldsymbol{Z}_p[[\Gamma]]$ with the power series ring $\Lambda = \boldsymbol{Z}_p[[T]]$ by $\gamma = 1 + T$. We regard several groups associated to k_∞ as modules over Λ or $\Lambda[\Delta]$ by this identification. It is known that $\mathrm{Gal}(M/N)$ and $\mathfrak{X}$ are finitely generated and torsion over Λ (cf. [13, Theorem 5]). For a finitely generated torsion Λ-module X, we denote by $\mathrm{char}(X)$ its characteristic polynomial, which is a uniquely determined distinguished polynomial times p^μ with $\mu \geq 0$.

Let v be a prime divisor of k_n over p and $k_{n,v}$ the completion of k_n at v. Let $\mathfrak{U}_{n,v}$ be the group of principal units of $k_{n,v}$ and let $\mathfrak{U}_n = \prod_{v\mid p} \mathfrak{U}_{n,v}$ be the group of semi-local units of k_n at p, where v runs over all prime divisors of k_n over p. Embedding E_n into $\prod_{v\mid p} k_{n,v}^\times$ diagonally, we denote by $\mathfrak{E}_n$ the completion of $E_n \cap \mathfrak{U}_n$ in $\mathfrak{U}_n$. Let $\mathfrak{U}_\infty$ and $\mathfrak{E}_\infty$ be the projective limits of $\mathfrak{U}_n$ and $\mathfrak{E}_n$ with respect to the relative norms, respectively:

$$\mathfrak{U}_\infty = \varprojlim \mathfrak{U}_n, \qquad \mathfrak{E}_\infty = \varprojlim \mathfrak{E}_n.$$

The groups $\mathfrak{U}_\infty$ and $\mathfrak{E}_\infty$ are regarded as modules over $\Lambda[\Delta]$. By class field theory, the inertia group $\mathfrak{I}^- = \mathrm{Gal}(M^-/L^-)$ of M^- is canonically isomorphic to $\mathfrak{U}_\infty^-/\mathfrak{E}_\infty^-$ over $\Lambda[\Delta]$ (cf. [3, Theorem 1]):

$$\mathfrak{I}^- \cong \mathfrak{U}_\infty^-/\mathfrak{E}_\infty^-. \tag{9}$$

Proof of Proposition 2(b). Let κ be the p-adic unit such that $\xi^\gamma = \xi^\kappa$ for all $\xi \in \mu_{p^\infty}$. For the torsion Λ-submodule $\mathrm{Tor}_\Lambda \mathfrak{U}_\infty^-$ of $\mathfrak{U}_\infty^-$, it is known that $\mathrm{char}(\mathrm{Tor}_\Lambda \mathfrak{U}_\infty^-)$ is a power of $\dot{T} = T - (\kappa - 1)$ (cf. [13, Theorem 25]). Hence, so is $\mathrm{char}(\mathrm{Tor}_\Lambda \mathfrak{I}^-)$ by (9) because $\mathfrak{E}_\infty^-$ is torsion over Λ and $\mathrm{char}(\mathfrak{E}_\infty^-)$ divides $\dot{T}$ (cf. [15, Theorem 4.12]). On the other hand, it is known (cf. [6, pp. 265–266]) that $\mathrm{char}(\mathfrak{X}^+)$ is relatively prime to T because the Leopoldt conjecture holds for k and p by Brumer [1]. This implies that $\mathrm{char}(\mathrm{Gal}(M^-/N^-))$ is relatively prime to $\dot{T}$ by Proposition 2(a). From the above, we obtain $\mathrm{char}(\mathrm{Gal}(M^-/N^-L^-)) = 1$. This means that $\mathrm{Gal}(M^-/N^-L^-)$ is a finite Λ-submodule of $\mathfrak{G}^- = \mathrm{Gal}(M^-/k_\infty)$. Then, we must have $M^- = N^-L^-$ since $\mathfrak{G}$ has no nontrivial finite Λ-submodule (cf. [13, Theorem 18]). ∎

Proof of Proposition 3(b). This is proved in a way similar to Proposition 2(b). ∎

5. PROOF OF PROPOSITION 4

5.1. *Some Lemmas*

Let $k/\boldsymbol{Q}$ be an imaginary abelian field with $\zeta_p \in k$ and $p \nmid [k:\boldsymbol{Q}]$. We use the same notation as before. We identify the completed group ring $e_{\Psi^*}\boldsymbol{Z}_p[\Delta][[\Gamma]]$ with the power series ring $\Lambda_O = O[[T]]$ by $\gamma = 1 + T$ and the identification $O = e_{\Psi^*}\boldsymbol{Z}_p[\Delta]$ in Section 3.1. Hence, for a $\boldsymbol{Z}_p[\Delta][[\Gamma]]$-module X, its Ψ^*-component $X(\Psi^*)$ is regarded as a Λ_O-module. To prove Proposition 4, we need the following two lemmas.

LEMMA 1. *When $\psi(p) \neq 1$ (resp. $\psi(p) = 1$), the Galois group $\mathfrak{H}(\Psi^*) = \mathrm{Gal}(N(\Psi^*)/k_\infty)$ is isomorphic to a submodule of Λ_O (resp. $\Lambda_O \oplus \Lambda_O/(\dot{T})$) with a finite index.*

LEMMA 2 (cf. Gillard [5, Proposition 1]). *When $\psi(p) \neq 1$ (resp. $\psi(p) = 1$), $\mathfrak{U}_\infty(\Psi^*)$ is isomorphic to Λ_O (resp. $\Lambda_O \oplus \Lambda_O/(\dot{T})$).*

Let E'_n be the group of p-units of k_n. We put

$$N' = \bigcup_n k_\infty(\epsilon^{1/p^{n+1}} \mid \epsilon \in E'_n).$$

The Λ-module structure of $\mathrm{Gal}(N'/k_\infty)$ is determined by [13, Theorem 15]. Because of the following claim, we can prove Lemma 1 exactly similarly to [13, Theorem 15] (see Remark 4) and we do not give its proof.

Claim. *We have $N'^- = N^-$.*

Proof. Let $E_{n,+}$ (resp. $E'_{n,+}$) be the group of units (resp. p-units) of k_n^+. We easily see that

$$N'^- = \bigcup_n k_\infty(\epsilon^{1/p^{n+1}} \mid \epsilon \in E'_{n,+})$$

from the Kummer duality (cf. [13, p. 276]). Let $\mathfrak{p}_i$ $(1 \leq i \leq r)$ be the prime ideals of k^+ over p, and let $h^+ = h'p^e$ be the class number of k^+ with $p \nmid h'$. We have $\mathfrak{p}_i^{h'p^e} = (\alpha_i)$ for some p-unit $\alpha_i \in k^+$. We see that $E_{n,+} \cdot \langle \alpha_i \mid 1 \leq i \leq r \rangle$ is of finite index in $E'_{n,+}$ since $\mathfrak{p}_i$ is totally ramified in k_n^+/k^+. Therefore, we obtain

$$N'^- = \bigcup_n k_\infty(\epsilon^{1/p^{n+1}},\ \alpha_i^{1/p^{n+1}} \mid \epsilon \in E_{n,+},\ 1 \leq i \leq r). \tag{10}$$

Denote by $\mathfrak{p}_{i,n}$ the unique prime ideal of k_n^+ over $\mathfrak{p}_i$. Then, we have $\mathfrak{p}_{i,n}^{h'p^{e+n}} = (\alpha_i)$. It is known (cf. [6, p. 267]) that $\mathfrak{p}_{i,n}^{h'}$ is capitulated in k_m^+ for sufficiently large $m > n$ because the Leopoldt conjecture holds for k_n^+ and p. Therefore, we obtain

$$\alpha_i = \epsilon\alpha^{p^{n+e}}$$

for some $\epsilon \in E_{m,+}$, $\alpha \in k_m^+$, and some m. From this and (10), we obtain the assertion. ∎

Remark 4. To prove Lemma 1 similarly to [13, Theorem 15], all we have to do is to repalce the formula of the seventh line of [13, p. 281] by

$$(E'_n \otimes \boldsymbol{Q}_p/\boldsymbol{Z}_p)(\Psi) = (E'_{n,+} \otimes \boldsymbol{Q}_p/\boldsymbol{Z}_p)(\Psi) \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^{(p^n+\delta)\deg(\Psi)} \tag{11}$$

with $\delta = 0$ or 1 according as $\psi(p) \neq 1$ or $\psi(p) = 1$. Here, in the second term, we regard the even character Ψ as that of $\Delta^+ = \mathrm{Gal}(k^+/\boldsymbol{Q})$.

Let Z^+ be the decomposition group of p in k^+, and let $\alpha = \alpha_1$ be the element of k^+ defined in the proof of the claim. In the proof of the claim, we have seen that $E_{n,+} \cdot \langle \alpha^\sigma \mid \sigma \rangle$ is of finite index in $E'_{n,+}$, where σ runs over a complete set of representatives of Δ^+/Z^+. From this, we easily obtain the formula (11).

Remark 5. The assertion of Lemma 1 is also found in Sumida [14].

5.2. *Proof of Proposition* 4

Assume that $\psi(p) \neq 1$. In view of Lemma 1, let ι be an embedding of $\mathfrak{H}(\Psi^*)$ into Λ_O with a finite cokernel. By Proposition 3(b) and (9), we may regard the quotient $\overline{\mathfrak{U}}_\infty(\Psi^*) = \mathfrak{U}_\infty(\Psi^*)/\mathfrak{E}_\infty(\Psi^*)$ as a submodule of $\mathfrak{H}(\Psi^*)$, and we have $\mathfrak{Y}(\Psi^*) = \mathfrak{H}(\Psi^*)/\overline{\mathfrak{U}}_\infty(\Psi^*)$. We have $\mathfrak{E}_\infty(\Psi^*) = \{0\}$ since Ψ^* is odd and $\Psi^* \neq \omega$ (cf. [15, Theorem 4.12]), and hence

$$\overline{\mathfrak{U}}_\infty(\Psi^*) = \mathfrak{U}_\infty(\Psi^*) \cong \Lambda_O$$

by Lemma 2. So, the image $\iota(\overline{\mathfrak{U}}_\infty(\Psi^*))$ equals $f\Lambda_O$ for some $f \in \Lambda_O$. Therefore, we obtain an injection

$$\bar{\iota}\colon \mathfrak{Y}(\Psi^*) \longrightarrow \Lambda_O/(f).$$

Since the μ-invariant of $\mathfrak{X}$ is zero by [4], the above f is relatively prime to p. Therefore, by the above, we see that $\mathfrak{Y}(\Psi^*)$ is free over O.

Remark 6. We could not deal with the case $\psi(p) = 1$ because of the extra factor $\Lambda_O/(\dot{T})$ in $\mathfrak{Y}(\Psi^*)$ and $\mathfrak{U}_\infty(\Psi^*)$ (Lemmas 1, 2).

6. RELATED TOPICS

One says that a finite Galois extension L/K has a relative normal integral basis (NIB for short) when O_L is free (of rank one) over the group ring

$O_K[\mathrm{Gal}(L/K)]$. In [2], Childs proved the following:

THEOREM 4. *Let p be a prime number and let K be a number field with $\zeta_p \in K$. Let L/K be a cyclic extension of degree p. Then, L/K is unramified and has a NIB if and only if $L = K(\epsilon^{1/p})$ for some unit $\epsilon \in E_K$ satisfying*

$$\epsilon \equiv 1 \mod (\zeta_p - 1)^p. \tag{12}$$

Let K be a number field with $\zeta_p \in K$. We put

$$\mathcal{N}(K) = \{[\epsilon] \in E_K(K^\times)^p/(K^\times)^p \mid \epsilon \in E_K \text{ and satisfies (12)}\}.$$

For a unit $\epsilon \in E_K$, it is known (cf. [15, pp. 182–183]) that $K(\epsilon^{1/p})/K$ is unramified if and only if ϵ satisfies

$$\epsilon \equiv u^p \mod (\zeta_p - 1)^p$$

for some $u \in O_K$. Therefore, we have

$$\mathcal{N}(K) \subseteq \mathcal{E}(K) \subseteq \mathcal{H}(K).$$

This filtration is of interest because of Theorems 1 and 4.

Let $p \geq 3$ and let k be an imaginary abelian field with $\zeta_p \in k$. We assume that (i) $p \nmid [k : \boldsymbol{Q}]$ and that (ii) there is only one prime ideal of k over p. We write $\mathcal{N}_n = \mathcal{N}(k_n)$ for brevity. We have $\dim A_n^-/(A_n^-)^p = \lambda_k^-$ for all sufficiently large n by [4; 5, Corollary 13.29]. Hence, by the Kummer duality (3), we obtain $\dim \mathcal{H}_n^+ = \lambda_k^-$ for all sufficiently large n. In the previous papers [7–9], we have studied the quotient group $\mathcal{H}_n^+/\mathcal{N}_n^+$ in connection with Iwasawa theory.

Assume that $p \nmid h^+ = h(k^+)$ for a while. Then, it follows that $p \nmid h(k_n^+)$ from the assumptions on k (cf. [15, Theorem 10.4]). Therefore, we have

$$\mathcal{H}_0^+ = \mathcal{N}_0^+ \qquad \text{and} \qquad \mathcal{H}_n^+ = \mathcal{E}_n^+ \qquad \text{for } n \geq 1$$

by [10, Propositions 2, 3]. We proved in [8, Theorem 2(a)] that $\mathcal{E}_n^+ = \mathcal{N}_n^+$ when $(p-1)p^{n-1} \geq \lambda_k^-$. For relatively small n, there are examples of k with $\mathcal{E}_n^+ \neq \mathcal{N}_n^+$ (cf. [7, Example 2]).

When $p \mid h^+$, we have examples of k with $\mathcal{E}_n^+ \neq \mathcal{N}_n^+$ for all sufficiently large n (in contrast to the case $p \nmid h^+$) as we see below.

EXAMPLES. Let $p = 3$ and $k = \boldsymbol{Q}(\sqrt{d}, \sqrt{-3})$ with $d = 254$. We have $h^+ = 3, h^- = h(k)/h^+ = 12$. A fundamental unit of k^+ is $\epsilon = 255 + 16\sqrt{254}$. It is known that $\lambda_k^- = 1$ and $\lambda_k^+ = 0$ by [11]. Note that

$$\epsilon^8 \not\equiv 1 \mod (\zeta_3 - 1)^3. \tag{13}$$

Therefore, we see that $\mathcal{E}_0^+ = \mathcal{N}_0^+ = \{0\}$. We also see from the above and (3) that $\mathcal{H}_0^+ = \langle [\alpha] \rangle$ for some $\alpha \in k^+$ with $(\alpha) = \mathfrak{A}^3$, where $\mathfrak{A}$ is a *nonprincipal* ideal of k^+. Since $\lambda_k^- = 1$, we have $\mathscr{H}_n^+ = \langle [\alpha] \rangle$ for all n. By [11], the ideal $\mathfrak{A}$ is capitulated in k_n^+ with $n = 5$; i.e., $\mathfrak{A} = (\beta)$ for some $\beta \in k_5^+$. From this, we obtain $\mathscr{H}_n^+ = \mathscr{E}_n^+$ for $n \geq 5$. On the other hand, we see that $\mathscr{N}_n^+ = \{0\}$ for all n from (13) and $\lambda_k^- = 1$ by virtue of [9, Proposition 1]. Thus, we obtain $\mathscr{E}_n^+ \neq \mathscr{N}_n^+$ for $n \geq 5$. In a similar way, we see that $\mathscr{E}_n^+ \neq \mathscr{N}_n^+$ for $n \geq 1, 2, 3, 4$ when $d = 761, 443, 785, 2666$, respectively, by using the data given in [11].

REFERENCES

1. A. Brumer, On the units of algebraic number fields, *Mathematika* **14** (1967), 121–124.
2. L. Childs, The group of unramified Kummer extensions of prime degree, *Proc. London Math. Soc.* **35** (1977), 407–422.
3. J. Coates, p-adic L-functions and Iwasawa theory, *in* "Algebraic Number Fields" (A. Fröhlich, Ed.), pp. 263–353, Academic Press, London, 1977.
4. B. Ferrero and L. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, *Ann. Math.* **109** (1979), 377–395.
5. R. Gillard. Unités cyclotomiques, unités semi-locales et $\mathbf{Z}_\ell$-extensions II, *Ann. Inst. Fourier* **29** (1979), 1–15.
6. R. Greenberg. On the Iwasawa invariants of totally real number fields, *Amer. J. Math.* **98** (1976), 263–284.
7. H. Ichimura, On a relative normal integral basis problem over abelian number fields, *Proc. Japan Acad.* **69** (1993), 413–416.
8. H. Ichimura, On p-adic L-functions and normal bases of rings of integers, *J. Reine Angew. Math.* **462** (1995), 169–184.
9. H. Ichimura, On a normal integral bases problem over cyclotomic $\mathbf{Z}_p$-extensions, *J. Math. Soc. Japan* **48** (1996), 689–703.
10. H. Ichimura, On power integral bases of unramified cyclic extensions of prime degree, *J. Algebra*, to appear.
11. H. Ichimura and H. Sumida, On the Iwasawa invariants of certain real abelian fields, *Tohoku Math. J.* **49** (1997), 203–215.
12. H. Ichimura and H. Sumida, On the Iwasawa invariants of certain real abelian fields II, *Internat. J. Math.* **7** (1996), 721–744.
13. K. Iwasawa, On $\mathbf{Z}_l$-extensions of algebraic number fields, *Ann. Math.* **98** (1973), 246–326.
14. H. Sumida, Initial layers of $\mathbf{Z}_p$-extensions and Greenberg's conjecture, *Manuscripta Math.* **98** (1999), 477–490.
15. L. Washington, "Introduction to Cyclotomic Fields," 2nd ed., Springer-Verlag, New York, 1996.